ObservePoint

COOKIE CHEAT SHEET

WHAT'S A COOKIE?

A persistent piece of information given by a website to your browser and stored on your computer's hard drive until it expires. Cookies allow websites to identify return visitors.

WHAT DOES A COOKIE LOOK LIKE?

A cookie is a name-value pair. The name and value are text. Cookies have other metadata like expiration dates, security policies, and which websites are allowed to access the cookie.

WHERE ARE COOKIES STORED ON YOUR HARD DRIVE?

This varies by browser. For Chrome, they are stored in a single file on your hard drive.

- On **Windows**, the file is located in: C:\Users\<your_username>\AppData\Local\Google\Chrome\User Data\Default\Cookies.
- For **Mac**, the file is: ~/Library/Application Support/Google/Chrome/Default/Cookies.

The file is an **SQLite** database file and can be queried with SQL commands.

WHAT'S THE DIFFERENCE BETWEEN A 1ST-PARTY COOKIE AND A 3RD-PARTY COOKIE?

- **1st-party:** A cookie that has the same domain as the website you're visiting, used for features like logins, shopping carts, preferences.
- **3rd-party:** A cookie with a domain that is not the same domain as the website you're visiting, used primarily to identify users across websites for tracking and advertising.

WHAT COOKIE METADATA SHOULD YOU PAY ATTENTION TO?

Domain: The domain instructs the browser to send the cookies associated with that domain whenever you visit that website. The browser will not send cookies to websites with a different domain.

Secure: This flag instructs the browser to send these cookies only over a secure channel (HTTPS). Modern cookies should all be secure.

HTTPOnly: Tells cookies to send information only over a network request and doesn't allow JavaScript code to read the cookie's content. Protects against a class of security vulnerabilities called **cross-site scripting (XSS)**.

SameSite: Defines whether browsers should include cookies in requests that go from one domain to another, like an image or form submission. Prevents malicious websites from impersonating users in a category of security vulnerabilities called **cross-site request forgery (CSRF)**.

Expiration: How long the cookie should stay on your hard drive, whether the cookie should expire at the end of your current browser session or a specific date in the future.

For more cookie details, **read the full blog post** from the webinar.